REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 1-8 are currently pending in the application; Claims 4, 5 and 6 are amended by the present amendment. Claims 4, 5 and 6 have been amended to correct minor informalities relating to antecedent basis. The specification and drawings have also been amended to correct typographical inaccuracies. Thus, no new matter is presented.

The Official Action presents the following issues: Claims 1, 2 and 4-7 were rejected under 35 U.S.C. § 102(e) as being anticipated by Yagawa et al. (U.S. Patent 6,751,598, hereinafter Yagawa); and Claims 3 and 8 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Yagawa.

The amendments to the specification and drawings submitted herewith were presented in a previous response filed on September 13, 2004. In response, an Advisory Action dated November 8, 2004 was issued which objected to the amendment on the grounds that it introduced new matter to the specification and the amendment was not entered. The Advisory Action stated that the modification of the term "tempered" to "tampered" introduced new matter to the application. Applicants respectfully traverse this assertion and maintain that amending the term "tempered" to "tampered" simply corrects a minor typographical error and does not introduce new matter to the application.

The present invention relates to a method and system for preventing an unauthorized user from performing an operation on "content data" or from "tampering" (or "to interfere with in a harmful manner") with the data. In this context, the term "tampered" accurately describes an unwanted operation that is, or might be performed on the content data. In contrast, the term "tempered" (or "to harden or strengthen (metal or glass) by application of heat or by heating and cooling") refers to a process that is generally used to harden a metal or

glass substance and has no applicability to the present invention. Further, the original specification at page 41, lines 6-9, describes that a program displays a message stating that "...the content may have be tampered" and "the content stored... is regarded as being tampered". Therefore, the term "tampered" was used in the original specification, in error, in the same context in which the word "tempered" was used in other portions of the original specification. Applicants respectfully submit that this amendment is made to correct a typographical error and does not introduce new matter into the specification and therefore should be entered.

Further, the specification has been amended so that the phrase "World Wide Ueb" has been corrected to read "World Wide Web", and Figure 6 has been amended so that the term "EUQAL" has been amended to read "EQUAL". These changes correct clear minor typographical errors, and therefore do not introduce new matter into the application.

Accordingly, Applicants respectfully submit that the amendments to the specification submitted in the present amendment do not introduce new matter into the specification and should be entered accordingly.

The outstanding Official Action asserts that Yagawa discloses all the limitations recited in Applicants' independent Claim 1. Applicants respectfully traverse this rejection.

Briefly recapitulating, the present invention provides a system and method that prevents data from being tampered with or copied in an unauthorized manner. In an exemplary embodiment, encrypted digital data is downloaded with management information including various parameters relating to the downloaded data. Among other parameters, the management information also includes usage rule parameters restricting the transfer and use of the digital data. The usage restrictions include limits on how many times the data can be copied, how many times the data can be transferred, etc.[1] These parameters form the basis

[1] Specification at pages 8-9.

for a calculated MAC value generated each time an "operation" is performed on the digital medium. Operations may include playing, recording, or transferring the digital data from one device to another (checked-in or checked-out).[2]

The MAC value is generated using the encryption key for the content device, as well as other possibly updatable calculation information which reflect the current status of the digital data.[3] Each time an operation is initiated on the digital file, the MAC value, which is currently stored in memory is compared to a newly calculated MAC value which is generated in response to the initiation of the operation. If the result of the comparison shows that the two MAC values differ, then the content of the digital file has been altered or the contents have been tampered with.[4] If tampering is detected then the use of the digital data is restricted.

Claim 1 recites, *inter alia*, an information processing apparatus, comprising:

> "...calculation means for performing a predetermined calculation on the basis of said encryption key and said calculation information, said calculation information including updatable information which is updated upon execution of a predetermined operation performed on said content data...
>
> control means for comparing the results of the calculation performed by said calculation means with a previous calculation result stored in said memory means and controlling use of said content data stored in said storage means in accordance with the results of the comparison."

Yagawa describes a digital content distribution system and associated methodology of protecting distributed content. Specifically, Yagawa describes that a service program (23) which resides along with a key (21) in a ROM area (2) of a recording medium (1), the key is cooperatively utilized with content located in a RAM area (3) of the recording medium. The ROM area information is processed by a storage medium certification unit (43), a license

[2] Specification at page 37.
[3] Specification at page 37, lines 15-21.
[4] Specification at Figure 6.

agreement judging unit (44), a digital content execution unit (45), a digital content updating unit (46) and a customizing unit (47) of a storage medium driving device (41).

The storage medium certification unit is a processing block which judges whether or not the key exists in the ROM area of the storage medium and has a correct code. The license agreement judging unit judges whether or not the present use environment matches with a license agreement (22). The digital content execution unit fetches the digital content (31) from the RAM area (3) of the storage medium (1) and decodes the digital content.[5]

In operation, a command to execute the digital content (31) is sent from the input device (49) and the result of the execution is displayed on the display device (48). The digital content updating unit (46) makes a request for the latest addition (or version) of a digital content to the server machine (6) through the communication control unit (50) and the network (7) in accordance with the command from the input device (49) and stores the acquired digital content (31) into the RAM area (3). The customizing unit (47) is a processing block which performs the input of the data into the user profile code field (32) of the RAM area (3) and the updating of data and user profile code field (32) in accordance with the command and data inputted from the input device (49).

The Advisory Action of November 8, 2004, cites the portion of Yagawa that "discusses the number of times of distribution" of content data and that the description of such an operation teaches "calculation information including updatable information which is updated upon the execution of a predetermined operation on the content data", as recited in Claim 1.[6] Specifically, Yagawa describes that the distribution control unit (63) is able to check the number of times specific content has been distributed (steps 638-640) and control

[5] Yagawa at column 6 lines 30-42.
[6] Advisory Action of November 8, 2004 at page 2.

the distribution of the content based on whether this number is greater than or equal to a predetermined number of permitted distributions.[7]

However, Claim 1 further recites a calculation means for performing a predetermined calculation on the basis of an encryption key and calculation information which includes updatable information which is updated upon execution of a predetermined operation performed on the content data. This feature was not addressed in the Advisory Action of November 8, 2004, and is not disclosed in Yagawa.

Yagawa fails to describe that an encryption key is used in a calculation with any of the parameters included in the management information; much less any parameter which is updatable upon the execution of a predetermined operation on the content data. Specifically, Yagawa describes that a storage medium certification unit (43) fetches the key (21) from the storage location (A) and discriminates the key through the comparison with the key attached to digital content (31) or embedded in the program (23).[8] Therefore, Yagawa describes that the key to be used is matched with the key included in the digital content and used to decrypt the digital content itself, but Yagawa fails to teach or disclose that the key is used in a calculation with information that is updated upon an operation on the content data. Thus, Yagawa fails to teach or disclose performing a predetermined calculation on the basis of the encryption key and the calculation information which includes updatable information which is updated upon the execution of a predetermined operation performed on the content data, as recited in Claim 1.

Claim 1 further recites comparing the results of the predetermined calculation with a previous calculation result and controlling the use of the content in accordance with the result of the comparison. As discussed above, Yagawa describes controlling the use of the content based on the number of times that the data has been distributed, or whether the recording

[7] Yagawa at Figure 8, and column 11, lines 23-35.
[8] Yagawa at column 8 lines 48-56.

medium contains the appropriate key code or licensing agreement to receive the content data.[9] However, Yagawa fails to teach or disclose comparing the result of a predetermined calculation performed on the basis of the encryption key and updatable information, which is updated upon a predetermined operation performed on the content data, to a previously stored calculation and controlling the use of the content in accordance with the result of the comparison, as recited in Claim 1.

Accordingly, Applicant respectfully requests that the rejection of Claim 1 under 35 U.S.C. § 102(e) be withdrawn. For substantially the same reasons as given with respect to Claim 1, it is also submitted that amended Claims 4, 5 and 6 patentably define over Yagawa. As Claims 3 and 8 depend from Claims 1 and 7 respectively it is submitted that these claims also patentably define over Yagawa for at least the reasons cited above.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1-8 is patentably distinguishing over the prior art. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\ATH\PROSECUTION\20'S\203742-US\203742 AM-RCE.DOC

[9] Yagawa at column 6 lines 30-42, and Figure 8, and column 11, lines 23-35.

IN THE DRAWINGS

The attached sheet of drawings includes changes to Fig. 6. This sheet, which includes Fig. 6, replaces the original sheet including Fig. 6.

Attachment: Replacement Sheet